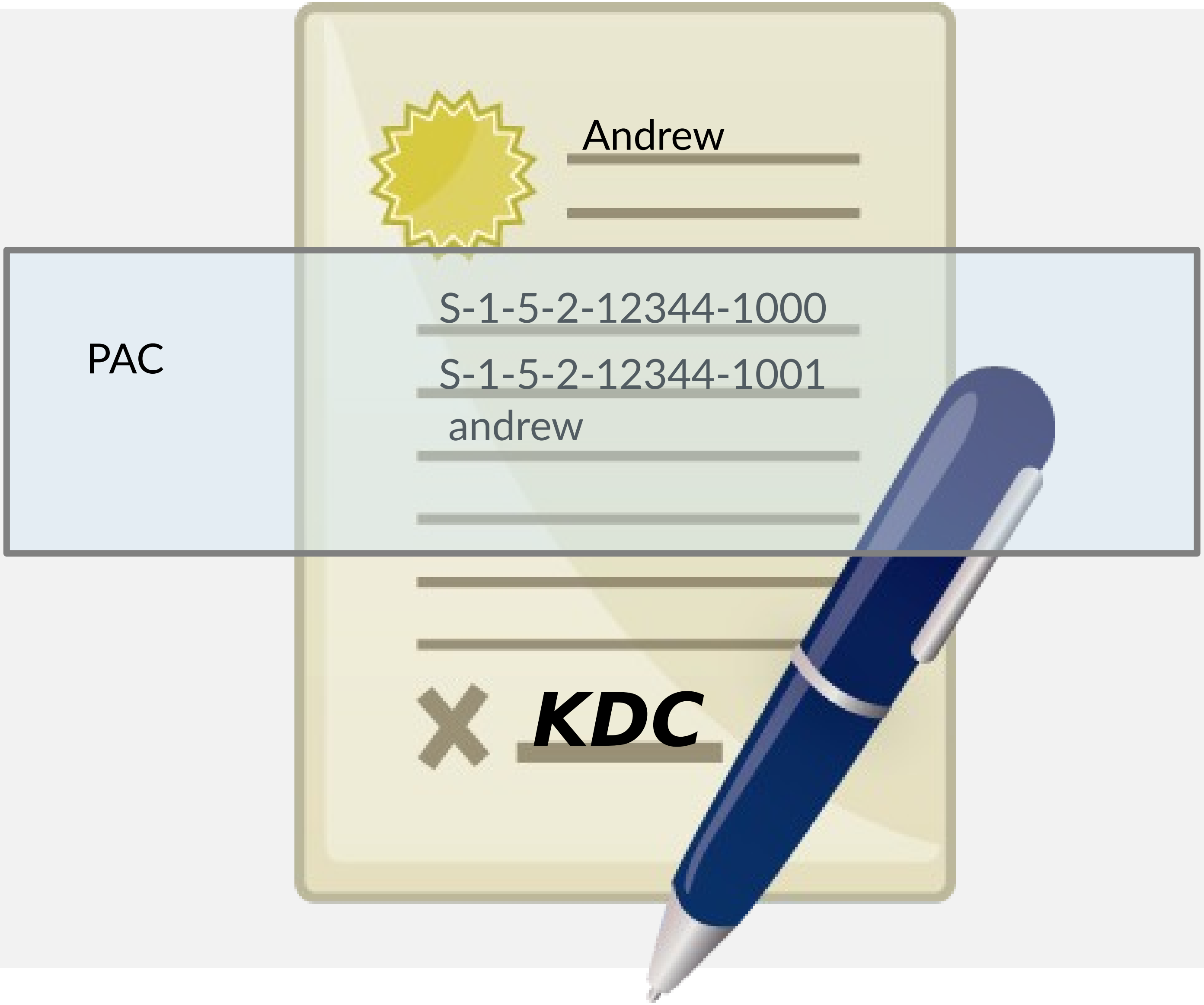
Breaking AD (and clients): the dollar ticket attack

Or fun and profit with fully documented features!

catalyst
expert open source solutions

SAMBA
TEAM

https://commons.wikimedia.org/wiki/File:Singapore_coins_in_a_stack.jpg



Andrew

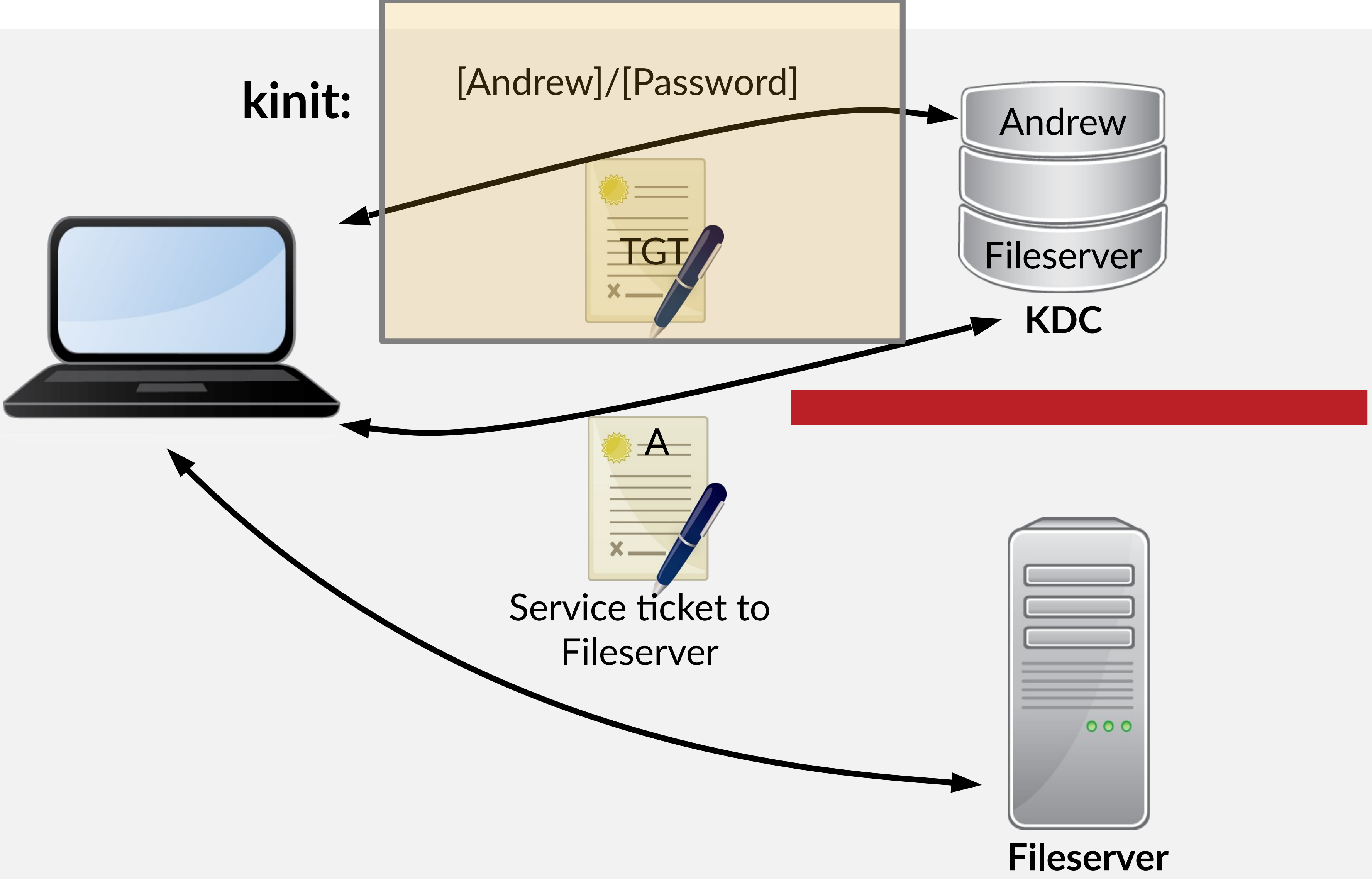
PAC

S-1-5-2-12344-1000

S-1-5-2-12344-1001

andrew

KDC


kinit:
[Andrew]/[Password]
TGT
Andrew
Fileserver
KDC
A
Service ticket to Fileserver
Fileserver

Sadly:

A still-unaddressed security weakness in AD!

The setup

Windows 2022 (fully patched) AD DC

- with Certificate services for LDAPS support

Fedora 36 target

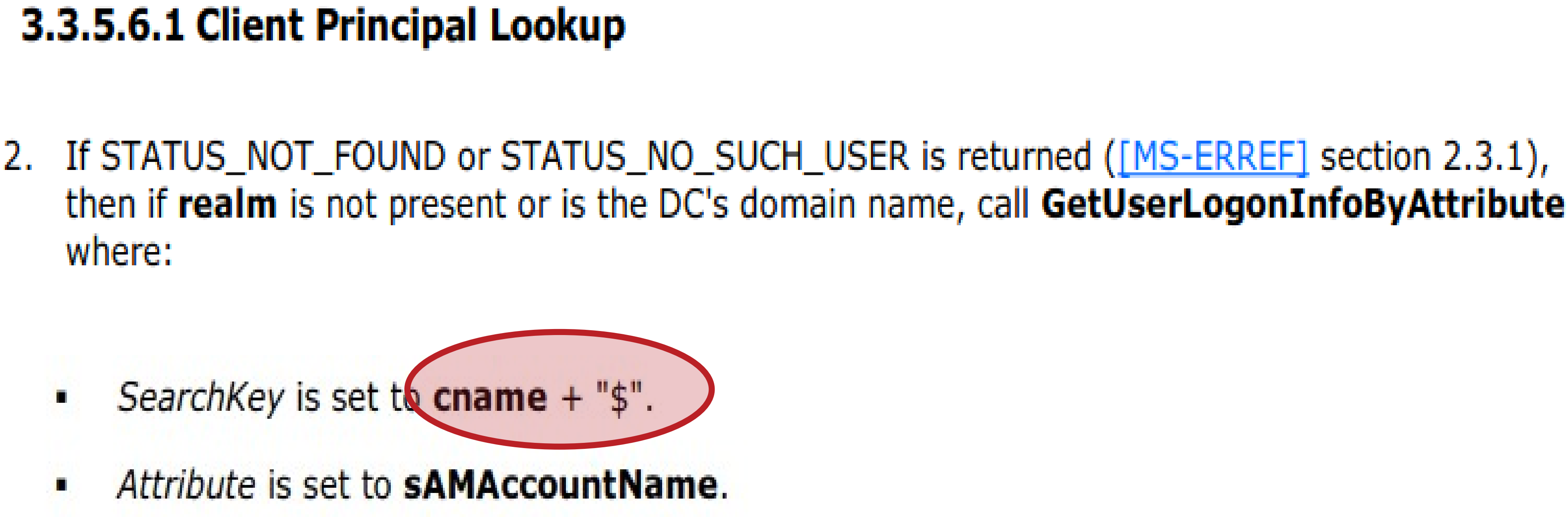
- joined to the AD domain

- **realm join -U administrator**
  win22.example.com –computer-name=fedora

<Exploit video omitted in PDF>

How did that happen: Just one more dollar!

Given an account in AD with a *harmless* name like **root$**



3.3.5.6.1 Client Principal Lookup

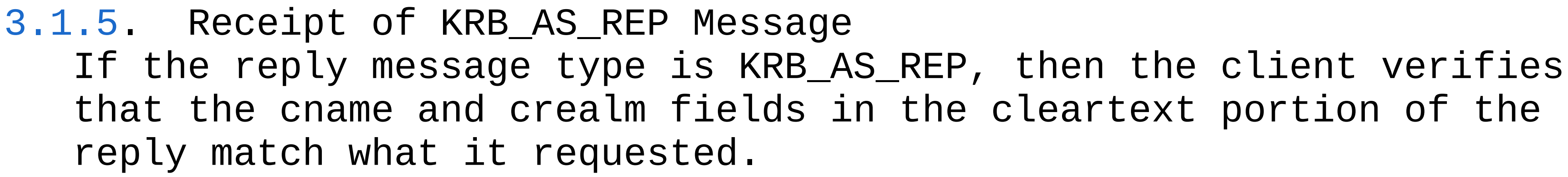
2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([MS-ERREF] section 2.3.1), then if **realm** is not present or is the DC's domain name, call **GetUserLogonInfoByAttribute** where:

    - *SearchKey* is set to **cname** + "$".
    - *Attribute* is set to **sAMAccountName**.

The ticket MUST come back exactly as the user requested (RFC 4120)

So: an account in the DB as **root$** can be accessed over Kerberos as **root**

This same name follows all the way to the target server!



3.1.5. Receipt of KRB_AS_REP Message

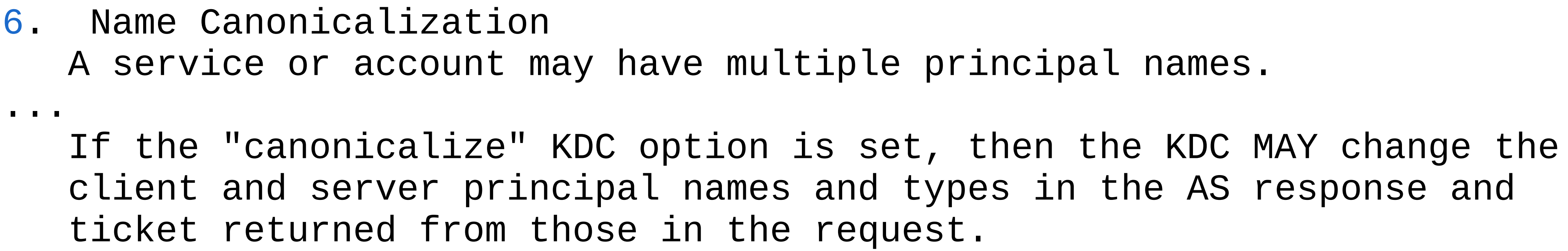
If the reply message type is KRB_AS_REP, then the client verifies
that the cname and crealm fields in the cleartext portion of the
reply match what it requested.

Must come back exactly – except with canonicalisation

AD Kerberos clients routinely specify optional "canonicalize" (RFC 6806)

This means the target (service accepting the ticket) gets samAccountName

...but also hides the other possibility from the developer!



```
6.  Name Canonicalization
   A service or account may have multiple principal names.
...
   If the "canonicalize" KDC option is set, then the KDC MAY change the
   client and server principal names and types in the AS response and
   ticket returned from those in the request.
```

Impacted services

NFS idmap – mapping principals to usernames - configured “nsswitch”

- all local names map name-wise to AD principals, including presumably **root** (from **root$**)

- Only **NFS-Ganesha** can read the **PAC** via Samba

SSH (as seen) and (eg) Apache mod_auth_kerb

Most of AD integration in Linux is re-purposed MIT Kerberos integration

All perfectly safe:
if only Administrators can add/modify users

Adding users and selecting names is NOT privileged in Windows AD

All users can (due machineAccountQuota):

- select a samAccountName (must end in $)
- rename the account to match an existing userPrincipalName

‘Helpdesk’ staff (the user who creates the account) can set:

- any samAccountName (including an existing userPrincipalName)
- any userPrincipalName (including an existing samAccountName)
- select names that might be sensitive outside AD (admin, root)

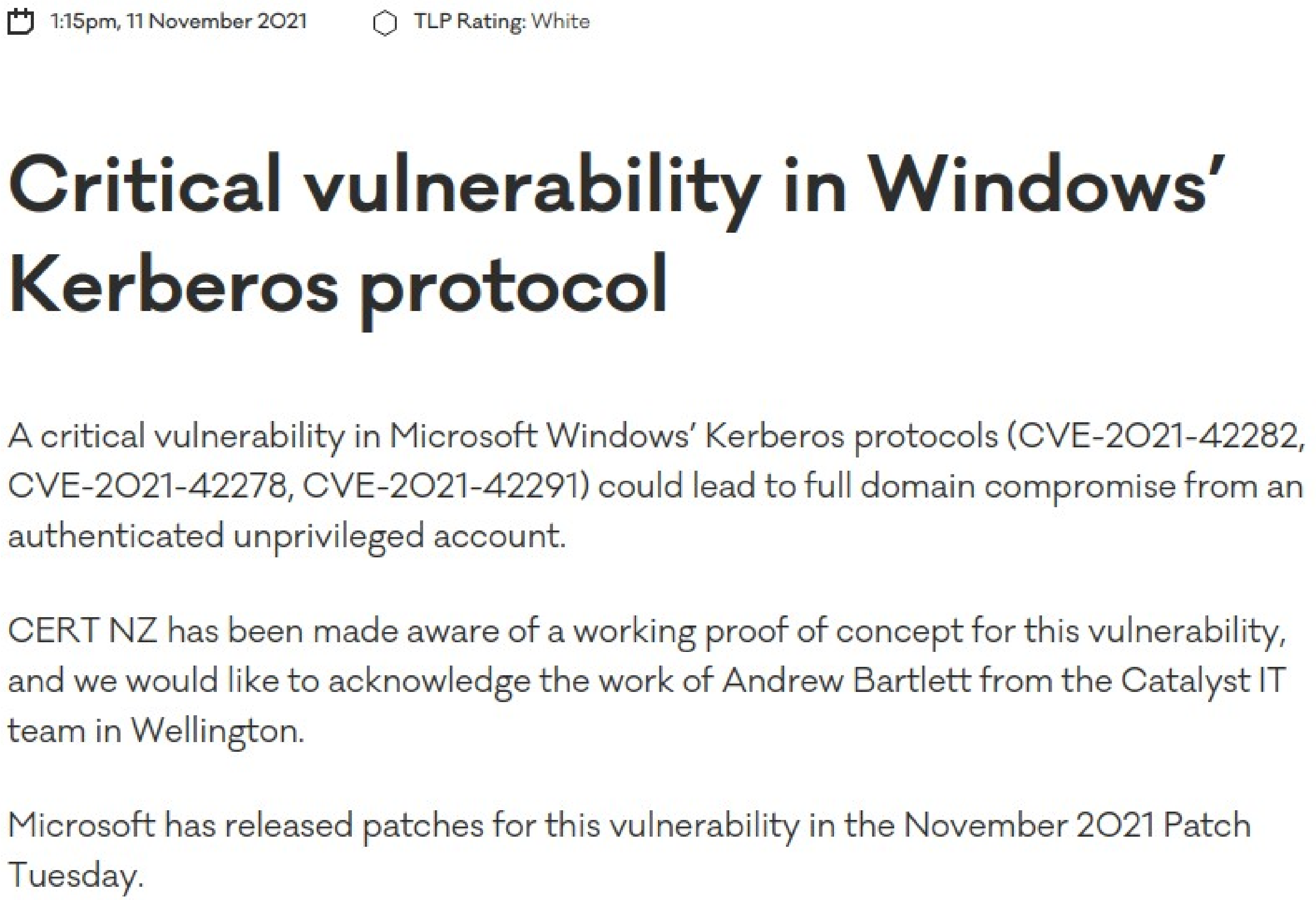
MIT-style Kerberos Targets are blind

Without parsing the PAC, the real username (samAccountName) is just not provided

Breaking AD

Actually Breaking Active Directory

- not just things using it



1:15pm, 11 November 2021 TLP Rating: White

Critical vulnerability in Windows' Kerberos protocol

A critical vulnerability in Microsoft Windows' Kerberos protocols (CVE-2021-42282, CVE-2021-42278, CVE-2021-42291) could lead to full domain compromise from an authenticated unprivileged account.

CERT NZ has been made aware of a working proof of concept for this vulnerability, and we would like to acknowledge the work of Andrew Bartlett from the Catalyst IT team in Wellington.

Microsoft has released patches for this vulnerability in the November 2021 Patch Tuesday.

Full domain takeover

Any user

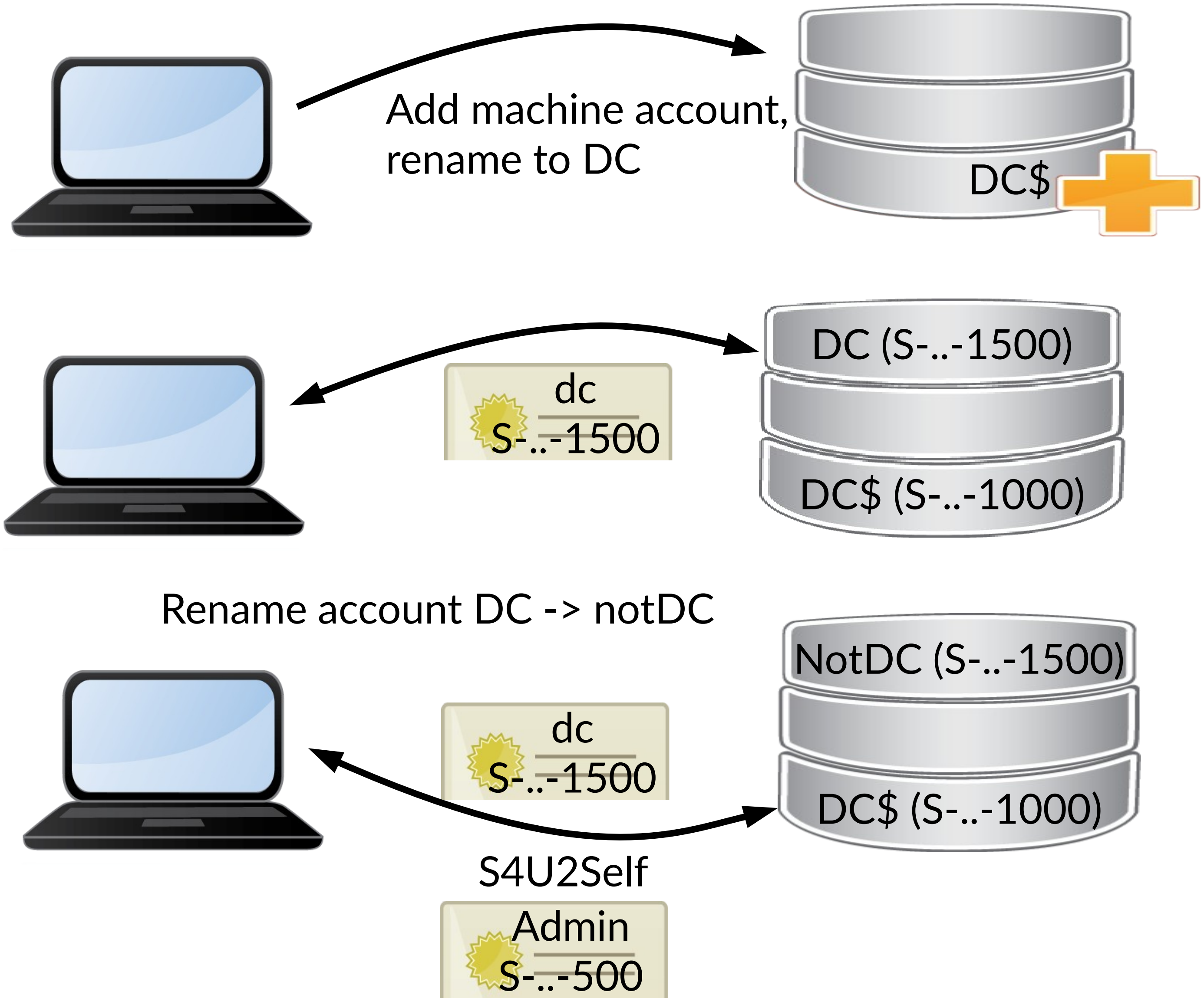
Any “service account”

Any computer, laptop, **kiosk**...

Could become **Domain Administrator**

Even on Samba :-(

CC-BY imamon https://flickr.com/photos/81506496@N00/283894146



Add machine account, rename to DC

DC$

DC (S-..-1500)

dc S-..-1500

DC$ (S-..-1000)

Rename account DC -> notDC

NotDC (S-..-1500)

dc S-..-1500

DC$ (S-..-1000)

S4U2Self

Admin S-..-500

How did this happen?

Historically Name based

- unique **string names** as authenticators
- administrated by **highly privileged** sysadmins

Active Directory added '**flexibility**' (complexity)

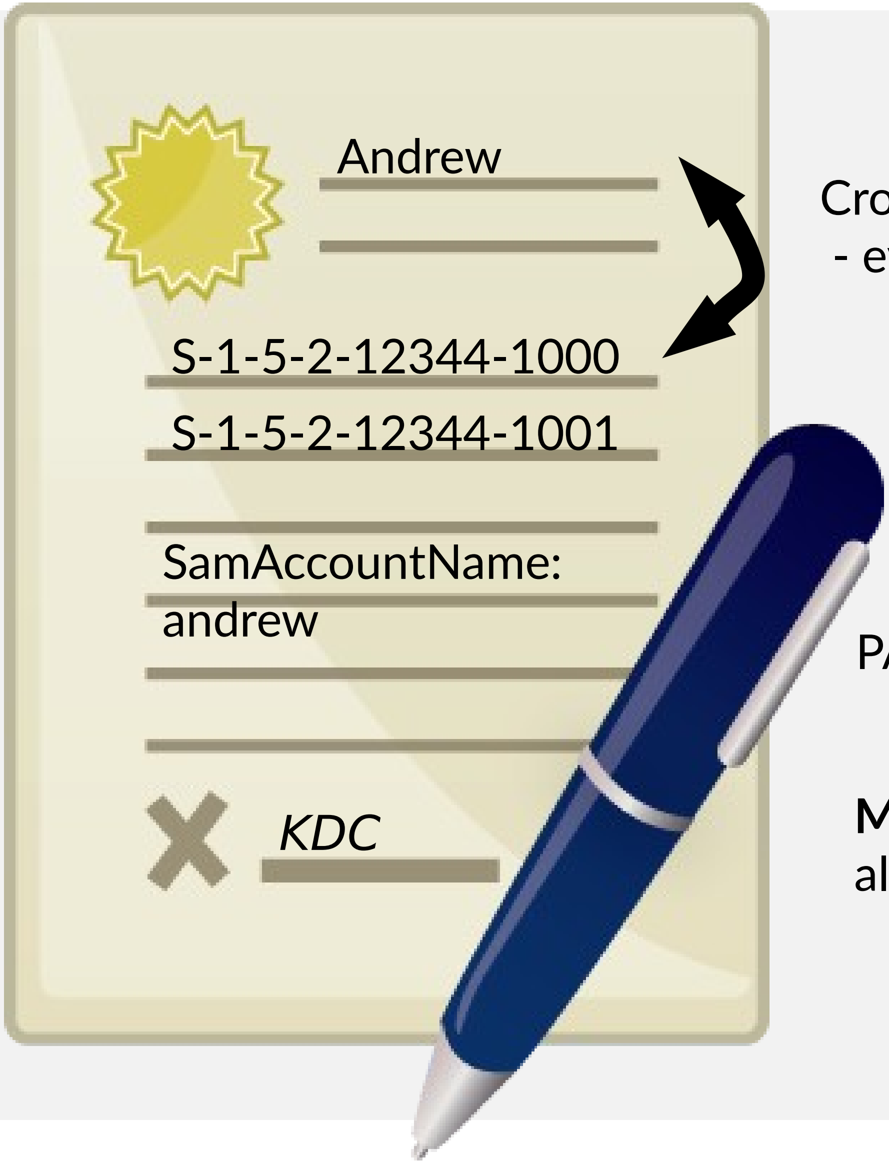
- Delegated administration (and MachineAccountQuota)
- Aliases
- Canonicalisation
- SIDs / PACs

But failure to use ONLY the SID leads to trusting untrustworthy names

WARNING: Always take in combination

In any security system, if you allow a login alias, you must canonicalise!

Never allow the end-user to choose their internal user identity



Cross-check Name with SID
 - every time

PAC becomes required in TGT

May 2022: X.509 Certificates also get a SID and are checked

Some mitigations for “MIT” clients also

The AD PAC now includes an easy-to-parse buffer with the SID and samAccountName

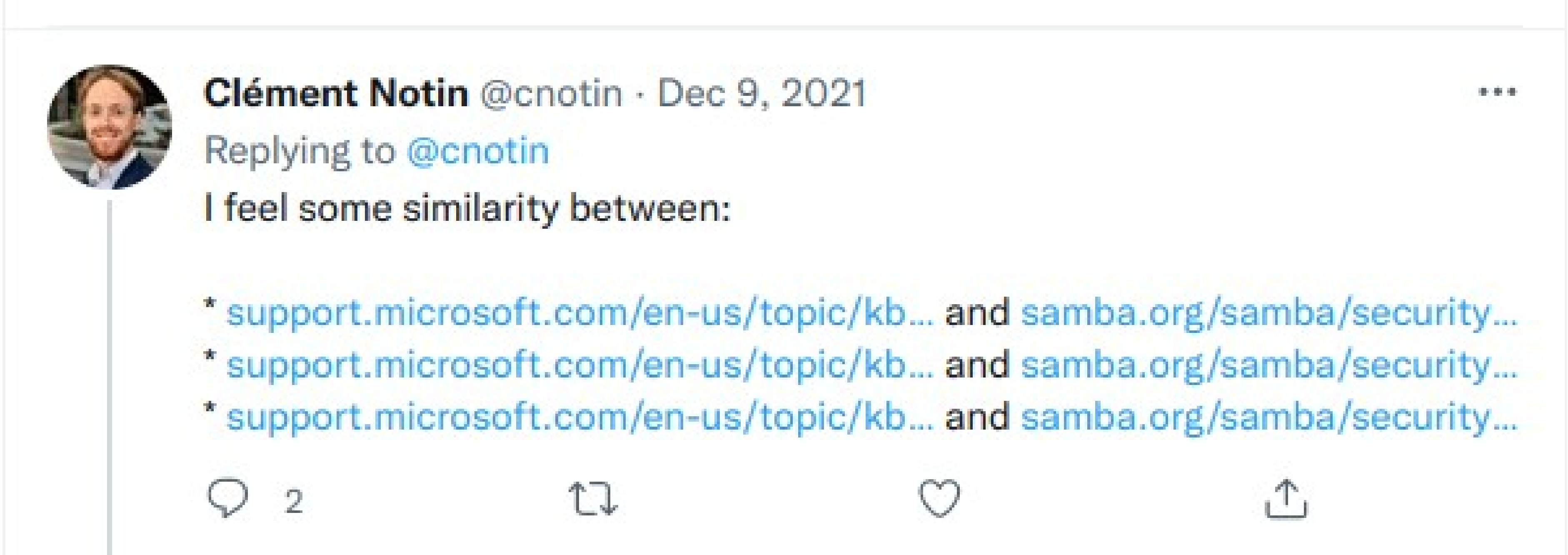
- Not NDR encoded, simple flag and length+offset parsing.

Sadly only unreleased Heimdal and SSSD can parse this so far

- Strong push-back against fixing *Microsoft’s bugs* on the client side
- Off by default

Need to find a way to have MIT Kerberos (in particular) to require a PAC and use it

- This in particular means finding a way to strongly indicate ‘we are in AD’
- On-by default – even in known AD domains - breaks installations as clients may request no-PAC

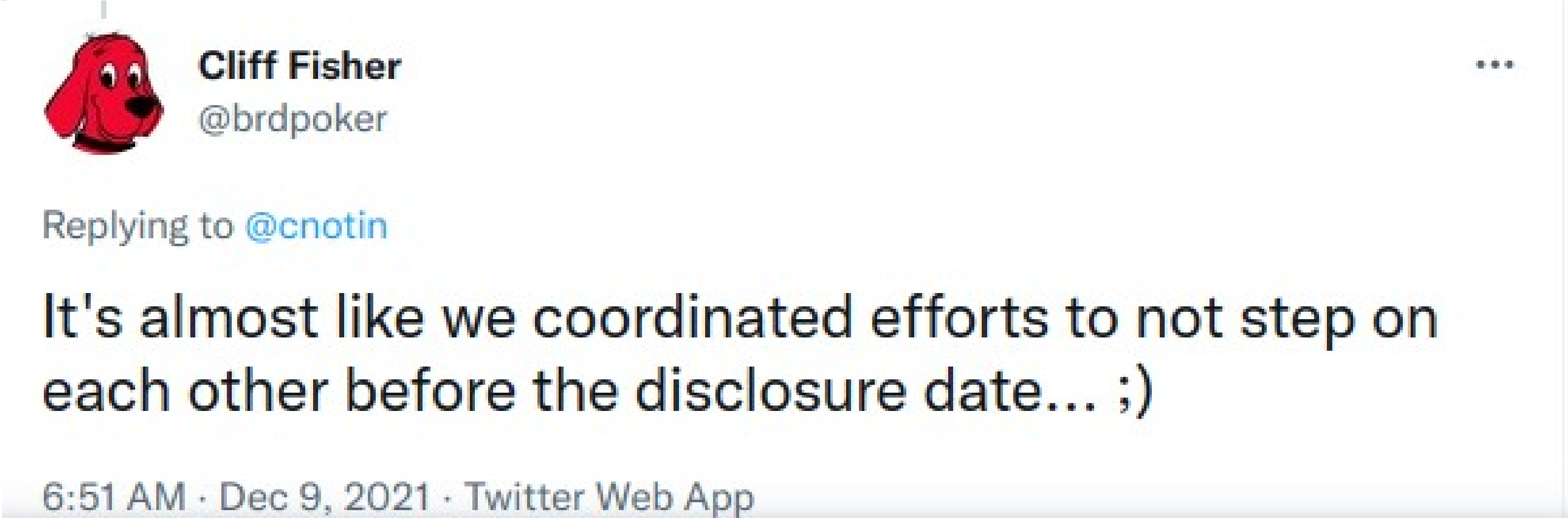


Clément Notin @cnotin · Dec 9, 2021

Replying to @cnotin

I feel some similarity between:

* support.microsoft.com/en-us/topic/kb… and samba.org/samba/security…
* support.microsoft.com/en-us/topic/kb… and samba.org/samba/security…
* support.microsoft.com/en-us/topic/kb… and samba.org/samba/security…



Cliff Fisher
@brdpoker

Replying to @cnotin

It's almost like we coordinated efforts to not step on each other before the disclosure date... ;)

6:51 AM · Dec 9, 2021 · Twitter Web App

The bad: I can’t save the world

Agreed a Samba/Microsoft release date of **Nov 9 2021**

I raised the PKINIT issues now known as “Certifried” with MS on the calls

- Waiting to fix those would have taken until **May 2022**

I also agreed to a release with **no coordinated plan** for “MIT” clients

In the end we had to protect our AD customers and **my own sanity**

- Also one can’t keep applying employer resources forever

The ugly: Please help – need advocacy to get change

Need further change to Active Directory behaviour to close this properly:

- Refuse TGT without canonicalise
- Always send the PAC to the target server?

But all this needs industry consensus on the ‘call’ for a change

- In particular MS is unlikely to do more unless targets commit to using it
- Perhaps some action if this is shown to be a real ongoing **threat**

Thanks

A big thankyou to the entire Samba Team that made this release possible

and to Catalyst for the space to chase “Andrew’s Kerberos Concerns” for so long

abartlet@catalyst.net.nz

abartlet@samba.org

catalyst.net.nz

samba.org

www.linkedin.com/in/
andrew-bartlett-samba

Funding thanks to:

univention
be open.

Hire Andrew @ catalyst